EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	123	"access node" and "mobile node" and "mobile terminal"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 09:44
S2	1	2003-485499.NRAN.	DERWENT	OR	ON	2007/07/21 19:06
S3	16	("20030190915" | "5793762" | "6104929" | "6137791" | "6151495" | "6195705" | "6256300" | "6442616" | "6606501" | "6622016" | "6628943" | "6643511" | "6711147" | "6725038").PN. OR ("6980801").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/21 19:07
S4	6	("20030144007" | "20030157936" | "20050136845" | "20060019694" | "6175550" | "6334059").PN. OR ("7233800").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/21 19:12
S5	70	("5063574" | "5291289" | "5748147" | "5757766" | "5771224" | "5822323" | "5848107" | "5952922" | "6009073").PN. OR ("6175550"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/21 19:25
S6	1	"20040240393"	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/21 20:17
S7	96	S1 and server	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 21:21
S8	3922	"Mobile IP"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 21:21

EAST Search History

S9	444	plurality near ("access node" "access router" "home agent")	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 18:33
S10	190	S8 and S9	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/21 21:25
S11	2	"6930988".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 09:03
S12	2	10/128253.app.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 13:22
S13	11	Zyren.IN.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 13:22
S14	2	"6553019".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/22 16:15
S15	2	10/128253.app.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 07:54

EAST Search History

S16	0	"10413415".app.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 07:55
S17	1	"10/413415".app.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 08:16
S18	2	"7020120".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 08:30
S19	2	"6636498".pn.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 09:33
S20	3153	Hancock.In.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 09:33
S21	0	S20 and "readdresing a packet"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/25 18:32
S22	3	S20 and "mobile node"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 09:42

EAST Search History

S23	4702	370/392.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 09:43
S24	4636	370/389.ccls.	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 09:44
S25	149	S24 and "mobile node"	US-PGPUB; USPAT; USOCR; FPRS; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/07/23 09:45
S26	38	("4692918" | "5016244" | "5018133" | "5218600" | "5371852" | "5473599" | "5572528" | "5572582" | "5619552" | "5729537" | "5793762" | "5825759" | "5862345" | "6078575" | "6130892" | "6195705" | "6230012" | "6407988" | "6434134").PN. OR ("6636498"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 09:46
S27	3816	370/338.ccls.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 09:46
S28	1	"mobile node" and "access node" and "anchor node"	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 09:47
S29	2928	"mobile node"	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 09:47
S30	12	"access node" and "anchor node"	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 11:13
S32	1	"7203492".pn.	US-PGPUB; USPAT; USOCR	OR	ON	2007/07/23 11:14

IETF Mobile IP Working Group
INTERNET-DRAFT

Hesham Soliman, Ericsson
Claude Castelluccia, INRIA
Karim El-Malki, Ericsson
Ludovic Bellier, INRIA
July, 2002

Hierarchical MIPv6 mobility management (HMIPv6)
<draft-ietf-mobileip-hmipv6-06.txt>

Status of this memo

This document is a submission by the mobile-ip Working Group of the Internet Engineering Task Force (IETF). Comments should be submitted to the MOBILE-IP@STANDARDS.NORTELNETWORKS.COM mailing list.
This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that Other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at
http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at
http://www.ietf.org/shadow.html

Abstract

This draft introduces some extensions for MIPv6 and neighbour discovery to allow for the introduction of a Hierarchical MIPv6 mobility management model. The proposed hierarchical mobility management for MIPv6 will reduce the amount of signalling to CNs and the HA and may also improve the performance of MIPv6 in terms of handoff speed. Moreover, HMIPv6 is well suited to implement access control and handoffs between different access technologies.

TABLE OF CONTENTS

1. Terminology

This memo uses the terminology described in [1]. In addition, new terms are defined below:

Access Router (AR)	The Mobile Nodes default router located within a network operator s domain. The AR aggregates the outbound traffic of MNs.
Mobility Anchor Point (MAP)	A Mobility Anchor Point is a router located in a domain visited by the MN. The MAP acts as a local HA for the MN registered with it. Several MAPs can exist within a visited network.
Regional Care-of Address (RCoA)	An RCoA is an address obtained by the MN from the visited domain. An RCoA is an address on the MAPs subnet. It may be assigned to one of the MAPs interfaces (in the Extended mode of operation)or auto-configured by the MN when receiving the MAP option (Basic mode of operation).
HMIPv6-aware Mobile Node	An HMIPv6-aware MN is a MN that can receive and process the MAP option sent from Its default router and able to send a

MAP registration (Binding Update).

On-link CoA (LCoA) The LCoA is the on-link CoA configured on an MN s interface based on the prefix advertised by its default router. In [1] this is simply referred to as the Care-of-address. However, in this memo LCoA is used to distinguish it from the RCoA.

1. Introduction

This draft introduces the concept of a Hierarchical Mobile IPv6 network, utilising a new node called the Mobility Anchor Point (MAP).

In Mobile IPv6 there are no Foreign Agents, but there is still the need to provide a local entity to assist with MIP handoffs. Similar to MIPv4, Mobile IPv6 can benefit from reduced mobility signalling with external networks by employing a local Mobility Anchor Point. For this reason a new Mobile IPv6 node, called the Mobility Anchor Point (MAP), is used and can be located at any level in a hierarchical network of routers, including the Access Router (AR). Unlike FAs in IPv4, a MAP is not required on each subnet.

The MAP will limit the amount of Mobile IPv6 signalling outside the local domain and will support Fast Mobile IP Handovers to help Mobile Nodes in achieving seamless mobility (see Appendix A), as well as, supporting certain Mobile Network scenarios (see Appendix B). Other advantages of the introduction of the MAP functionality are covered in chapter 2.

Two different MAP modes are proposed in this memo, based on the usage of RCoA. A Mobile Node (MN) may use an RCoA as an alternate-care-of address (Extended mode) or form its own RCoA on the MAPs subnet (Basic mode) while roaming within a MAP domain. A MAP domain involves all access routers advertising the presence of a MAP. The two modes of operations are described in detail in chapters 5 and 6. In this memo, the MN s address obtained through the MAP (for both Basic and Extended modes) is referred to as the RCoA.

The aim of introducing the hierarchical mobility management model in

MIPv6 is to enhance the performance of MIPv6 while minimising the impact on MIPv6 or other IPv6 protocols.

2. Overview of HMIPv6

This Hierarchical MIPv6 scheme introduces a new function, the Mobility Anchor Point(MAP), and minor extensions to the MN and the Home Agent operations (for extended mode only). The CN operation will not be affected.

The introduction of the MAP concept minimises the latency due to handoffs between access routers since it will take less time to bind-update a local MAP than a distant HA. The coexistence of HMIPv6 and [4] is described in Appendix A.

Just like MIPv6, this solution is independent of the underlying access technology, allowing Fast Handoffs within, or between, different types of access networks. Furthermore, a smooth architectural migration can be achieved from Hierarchical MIPv4

networks, since a dual operation of IPv4 and IPv6 Hierarchies will be possible making use of the similarity in architecture.

The introduction of the MAP concept will further diminish signalling generated by MIPv6 over a radio interface. This is due to the fact that a MN only needs to perform one local BU(Binding Update) to a MAP when changing its layer 3 access point within the MAP domain. The advantage can be easily seen when compared to other scenarios (no MAP) where possibly two BUs will be sent (to one CN and HA).

The MAP will receive all packets on behalf of the MN it is serving and will encapsulate and forward them directly to the MN's current address. If the MN changes its current address within a local MAP domain (LCoA), it only needs to register the new address with the MAP. Hence, the global CoA (RCoA) registered with Correspondent Nodes (CNs) and the HA does not change. This makes the MN's mobility transparent to the CNs it is communicating with. The MAP can also be used to execute a Fast Handoff between ARs as described in Appendix A.

When using an RCoA, a MAP acts essentially as a local Home Agent (HA) for the MN, receiving its packets and tunnelling them to the MNs LCoA.
A MAP domain's boundaries are defined by the Access Routers (ARs) advertising the MAP information to the attached Mobile Nodes. The control of a MAP's mode of operation is left to the network administrator's discretion. A brief comparison between the two modes is shown in chapter 8 below.

The detailed extensions to MIPv6 and operations of the different nodes will be explained later in this document.

It should be noted that the MAP concept is simply an extension to the MIPv6 protocol. Hence an HMIPv6-aware MN with an implementation of MIPv6 SHOULD choose to use the MAP when discovering such capability in a visited network. However, in some cases the MN may prefer to simply use the standard MIPv6 implementation. For instance, the MN may be located in a visited network within its home site. In this case, the HA is located in the same site and could be used instead of a MAP. In this scenario, the MN would only update the HA whenever it moves. The knowledge of whether the HA is in the same site or not can be obtained as shown in [8].
Furthermore, a MN can, at any time, stop using the MAP. This provides great flexibility, both from a MN or a network operations point of view.

The network architecture shown below illustrates an example of the use of the MAP in a foreign network.

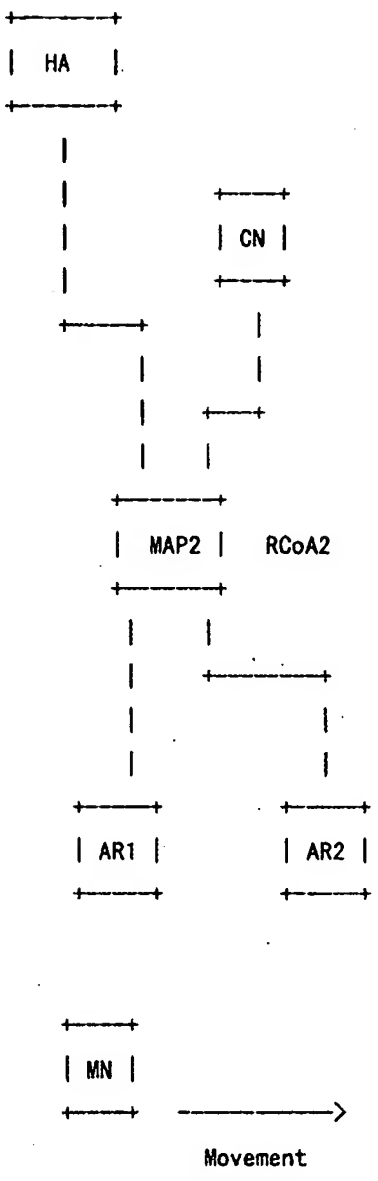


Figure 1: Hierarchical MIPv6 domain

In Figure 1, the MAP can help in providing seamless mobility for the MN as it moves from Access Router 1 (AR1) to Access Router 2 (AR2), while communicating with the CN. Although a multi-level hierarchy is not required for a higher performance, it is possible to use multi-level hierarchies of routers and implement the MAP functionality in AR1 and AR2 if needed. This would be required in cases where Mobile Routers are supported as will be explained later in chapter 7 and Appendix B. It should be noted that AR1 and AR2 could be two points of attachment in the same RAN (Radio Access Network) or in different RANs.

Upon arrival in a foreign network, the MN will discover the global address of the MAP. This address is stored in the Access Routers and communicated to the MN via Router Advertisements. The discovery phase will also inform the MN of the distance of the MAP from the MN. For example, the MAP function could be implemented as shown in Figure 1 and at the same time also in AR1 and AR2. In this case the MN can choose the first hop MAP or one further in the hierarchy of routers. The details on how to choose a MAP are provided in chapter 11.

A Router advertisement extension is proposed later in this document. The new MAP option in the router advertisement should inform MNs about the presence of the MAP (MAP discovery). This may also be used for MAP discovery by ARs and other MAPs which should advertise MAP options from all MAPs in the domain. A Router Renumbering [5] extension is also proposed for MAP discovery by ARs and other MAPs. If a router advertisement is used for MAP discovery, as described in this document, all ARs belonging to the MAP domain MUST advertise the MAP's IP address. The same concept should be used if other methods of MAP discovery are introduced in future.

The process of MAP discovery continues as the MN moves from one subnet to the next. As the MN roams within a MAP's domain, the same information announcing the MAP should be received. If a change in the advertised MAP's address is received, the MN MUST act on the change by sending the necessary Binding Updates to its HA and CNs.

If the MN is not HMIPv6-aware then the discovery phase will fail resulting in the MN using the MIPv6 [1] protocol for its mobility management. On the other hand, if the MN is HMIPv6-aware it SHOULD choose to use its HMIPv6 implementation. If so, the MN will first need to register with a MAP by sending it a BU containing its Home Address and on-link address (LCoA). In the case where the MN uses the MAP in Extended mode, the Home address used in the BU is the MNs Home Address on its Home subnet. On the other hand, if the MN is using a MAP in Basic mode, the Home address used in the BU is the RCoA. The MAP MUST store this information in its Binding Cache to be able to forward packets to their final destination when received from the different CNs or HAs.

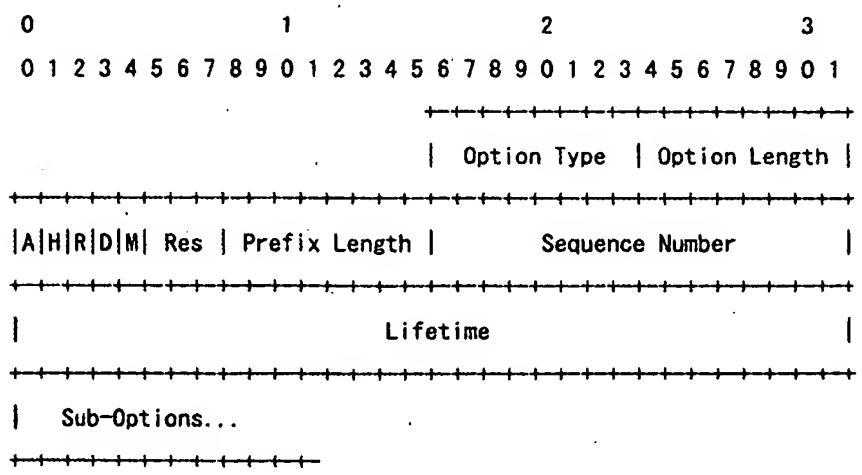
The MN will always need to know the original sender of any received packets. In the case where the MAP is used in Extended mode, all packets will be tunnelled by the MAP, hence the MN is not always able to determine whether the packets were originally tunnelled from the Home Agent (triangular routing) or received directly from a CN (route-optimised). This knowledge is needed by the MN to decide whether a BU needs to be sent to a CN in order to initiate route optimisation. For this purpose a check needs to be performed on the internal packet's routing header to find out whether the packet was tunnelled by the HA or originated from a CN using route optimisation instead. If a routing header exists in the internal packet, containing its RCoA and the MN's Home Address as the final destination, then route optimisation was used. Otherwise, triangular routing through the HA was used. This check on the routing header (as opposed to the check on the source of the tunnelled packets in [1]) can be used for both modes of operation as well as the standard operation described in [1].

To use the network bandwidth in a more efficient manner, a MN may decide to register with more than one MAP simultaneously and use each

MAP address for a specific group of CNs. For example, in Fig 1, if the CN happens to exist on the same link as the MN, it would be more efficient to use the first hop MAP (in this case assume it is AR1) for communication between them. This will avoid sending all packets via the "highest" MAP in the hierarchy and hence result in a more efficient usage of network bandwidth. The MN can also use its current on-link address (LCoA) as a CoA as specified in [1]. The knowledge of whether a CNs address belongs to the same site or not is outside the scope of this memo. However, [8] provides a mechanism for gaining this knowledge.

3. MIPv6 extension - Binding Update

This section outlines the extensions proposed to the BU option used by the MN in MIPv6. A new flag is added: the M flag that indicates MAP registration. When a MN registers with the MAP, the M flag MUST be set to distinguish this registration from a Home Registration or a BU being sent to a CN.

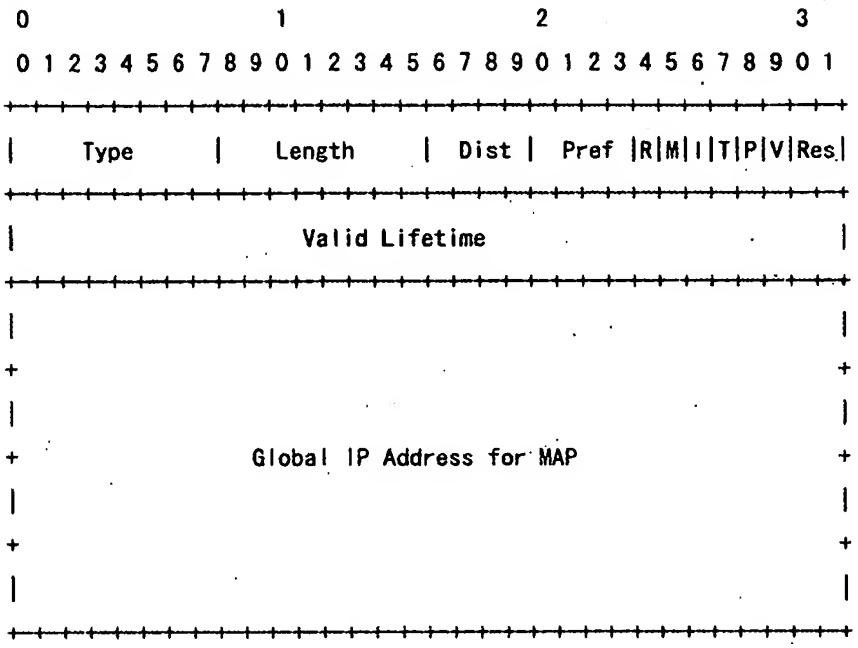


Description of extensions to the BU option:

M If set indicates a MAP registration.

4. Neighbour Discovery extension - The MAP option message format

The following figure illustrates the new MAP option.



Fields:

Type — Message type. TBA.

Length — 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value 0 is invalid. Nodes MUST silently discard an ND packet that contains an option with length zero.

Dist — A 4 bit unsigned integer showing the distance from the receiver of the advertisement. Its default value SHOULD be set to one if dynamic MAP discovery is used. The Distance MUST be set to one if the MAP is on the same link as the MN. This field need not be interpreted as the number of hops away from the MN. The only requirement is that the Distance field is consistently interpreted within one Domain. A Distance value of Zero MUST NOT be set.

Pref — The preference of a MAP. A 4 bit unsigned integer. A value of 15 indicates the lowest preference.

R — When set indicates that the MN MUST form an RCoA based on the prefix in the MAP option. If This flag indicates a Basic mode of operation.

M — When set indicates that the MN MUST use the

RCoA as an alternate-CoA. This indicates an Extended mode of operation. This flag MUST NOT be set when the R flag is set.

I When set indicates that the MN MAY use its RCoA as source address of its outgoing packets This flag MUST NOT be set if the R flag is not set.

T When set indicates that the on-link prefix is topologically incorrect. Hence the MN MUST use the MAPs CoA to be reached directly by the CN. This flag MUST only be set if the M flag is set. The flag indicates that the on-link prefix advertised for the MN is not topologically correct. This is particularly the case for Mobile networks and is explained in Appendix B.

P When set indicates that the MN MUST use its RCoA as source address of its outgoing packets This flag MUST NOT be set if the M flag is set.

V When set indicates that reverse tunnelling of outbound traffic, to the MAP, is allowed.

Valid Lifetime The minimum value (in seconds) of both, the preferred and valid lifetimes of the prefix assigned to the MAP s subnet. This value indicates the validity of the MAPs address

and consequently the time for which the RCoA is valid.

T

Global Address One of the MAP's global addresses. In the Basic mode of operation this address MUST have the prefix configured to be used for RCoA construction by the MN.

Although not explicitly included in the MAP option, the prefix length of the MAP s Global IP address MUST be 64. This prefix is the one used by the MN to form an RCoA (basic mode), by appending a 64-bit identifier to the prefix. Hence the need for having a static prefix length for the MAPs subnet.

To ensure a secure communication between routers, router advertisements, sent between routers for MAP discovery, SHOULD be authenticated by AH. In the case where this authentication is not possible (e.g. third party routers between the MAP and ARs), a network operator may prefer to manually configure all the ARs to send

the MAP option or use the router renumbering mechanism for MAP discovery, as shown in this document.

5. MAP discovery

This section describes how a MN obtains the MAP address and subnet prefix and how ARs in a domain discover MAPs. Two different methods for MAP discovery are defined below.
Dynamic MAP Discovery is based on propagating the MAP option from the MAP to the MN through certain (configured) router interfaces within the hierarchy of routers. This would require manual configuration of the MAP and the routers receiving the MAP option to allow them to propagate the option on certain interfaces.

Another method based on Router Renumbering [5] is also shown below. In this method, no manual configuration is required for routers within the domain. The MAP option is sent directly from a central node to all ARs within a MAP domain. This method is best suited to large networks where manually configuring all routers within a hierarchy maybe a significantly tedious operation. On the other hand, when using this method, any changes in the MAP option s parameters (e.g. preference) would require manual intervention.

5.1 Dynamic MAP Discovery

The process of MAP discovery can be performed in many different ways. In this document, router advertisements are used for the discovery phase by introducing a new option. The access router is required to send the MAP option in all router advertisements. This option includes the distance vector from the MN which may not imply the real distance in terms of the number of hops, the preference for this

particular MAP, the MAP's global IP address and the MAP's subnet prefix. In addition, the option contains some flags showing the MAPs mode of operation and other functions described throughout this document.

The ARs can be configured manually or automatically with this information. In this case, each MAP in the network needs to be configured with a default preference, the right interfaces to send this option on and the IP address to be sent. The initial value of the "Distance" field MAY be set to a default value of one. Upon reception of a router advertisement with the MAP option and given that a router is configured to re-send this option on certain interfaces, the router MUST copy the option and re-send it after incrementing the Distance field by one. If the router was also a MAP, it MUST send its own option in the same advertisement.
If a router receives more than one MAP option for the same MAP, from two different interfaces, it MUST choose the option with the smaller distance field.

In this manner, information about a MAP at a certain level in a hierarchy can be dynamically passed to a MN. Furthermore, by performing the discovery phase in this way, different MAP nodes are able to change their preferences dynamically based on the local policies, node overload or other load sharing protocols being used.

5.2 Using Router Renumbering for MAP discovery

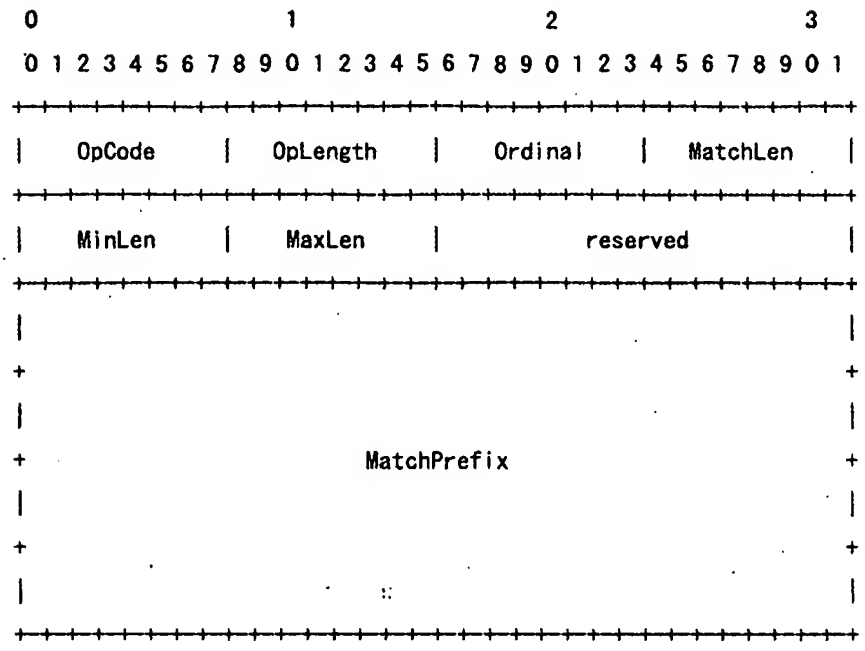
The Router Renumbering (RR) mechanism described in [5] defines a set of messages that can be used to renumber certain interfaces on a router without manual configuration of such router. RR messages are authenticated and protected against replay attacks. The same concept can be used to configure a router to propagate the MAP option on certain interfaces.

To be able to achieve this a new PCO command, PROPAGATE, is defined. This command is part of the Prefix Code Operation (PCO) and is included in the Match Prefix part of the message. A PCO message sent to a router with the PROPAGATE command MUST only contain one or more MAP options in the Use Prefix part of the message.

Upon reception of this message, a router will propagate the MAP option on the designated interface.

This mechanism can be used to configure ARs to advertise one or more MAP options. This is best suited to large networks or for cases where third party networks may exist between the MAP and ARs. Furthermore, unlike the Dynamic MAP discovery mechanism described earlier, this method does not require each router in the MAP domain to understand the MAP option.

5.2.1 Extension to the Match Prefix Part of RR



Extended Fields:

OpCode An unsigned 8-bit field specifying the operation to be performed when the associated MatchPrefix matches an interface's prefix or address. Values are:

1 the ADD operation

2 the CHANGE operation

3 the SET-GLOBAL operation

4 the PROPAGATE operation (new code).

5.3 MN Operations

When an HMIPv6-aware MN receives a router advertisement, it should search for the MAP option. One or more options may be found for different IP addresses or subnet prefixes.

A MN SHOULD register with the MAP having the lowest preference value. A MAP with a preference value of 15 SHOULD NOT be used in the MAP registration. A MN MAY however choose to register with one MAP over another depending on the value received in the Distance field, provided that the preference value is below 15.

If a MN has access to several ARs simultaneously, it SHOULD use an LCoA on the subnet defined by the AR that advertises its current MAP.

A MN MUST store the received option(s) and choose at least one MAP to register with. Storing the options is essential as they will be

compared to other options received later for the purpose of the move detection algorithm.

If no MAP options are found in the router advertisement, the MN MUST use the MIPv6 protocol as specified in [1].

If the M flag is set in the MAP option, the MN MUST register with the MAP using its Home Address in the Home address field in the BU.

If the R flag is set, the MN MUST use its RCoA as the Home Address when performing the MAP registration. RCoA is then bound to the LCoA in the MAPs Binding Cache.

If the I flag is set the MN MAY choose to use RCoA as a source address in its outgoing packets depending on whether location privacy (with respect to the CNs and HA) is required by the MN or user. This choice can be made by default policies in the MN or configurable options by the user.

If the P flag is set, the MN MUST use RCoA as a source address. This can be due to the network operator s requirements of not exposing certain prefixes to the external Internet.

A MN MAY choose to register with more than one MAP simultaneously or use both MAP address and its own address as CoAs simultaneously with different CNs provided the setting of the P and I flags allow such choices.

The V flag indicates that the MN is allowed to tunnel its outbound traffic to the MAP. This feature is useful for managing network mobility as will be described later in chapter 7.

5.4 MAP Operation for Dynamic MAP Discovery

When Dynamic MAP Discovery is used, the MAP discovery is done via router advertisements having the new MAP option added. A MAP will be configured to send its option or relay other MAPs' options on certain interfaces. The choice of interfaces is done by the network administrator and depends on the network architecture. A default preference value should be assigned to each MAP. It should be noted that a MAP can change its preference value at any time due to various reasons (e.g. node overload or load sharing). A preference value of 15 means that the MAP SHOULD NOT be chosen by a MN. This value could be reached in cases of node overload or node failures.

The MAP option is propagated down the hierarchy. Each router along the path to the access router will increment the Distance field by one. If a router that is also a MAP receives advertisements from other MAPs, it MUST add its own MAP option and propagate both options to the next level in the hierarchy.

6. Basic Mode: Supporting Mobile Nodes

This section defines a basic mode of HMIPv6 that can be used to support Mobile Nodes.
In the basic mode, the MN would have two addresses, an RCoA on the MAP's subnet and an on-link CoA (LCoA). This RCoA is formed in a stateless manner by combining the MAP's subnet prefix received in the MAP option with the MNs interface identifier.

As illustrated in this section, the basic mode is very simple in the sense that it only requires special treatment at the Mobile Nodes. The HA is unchanged. The MAP is merely a "local" HA that binds the MNs RCoA to an LCoA.

6.1 MN Operations

When a MN moves into a new MAP domain (i.e. its MAP changes), it needs to configure two CoAs:
An RCoA on the MAP's subnet and an on-link one (LCoA). These addresses are formed in a stateless manner.
After forming the RCoA based on the prefix received in the MAP option, the MN sends a BU to the MAP with the A, M and D flags set. The BU specifies its RCoA in the Home Address field. No alternate CoA sub-option is used. The LCoA is used as the source address of the BU). This BU will bind the MN's RCoA (similar to a Home Address) to its LCoA. The MAP (acting as a HA) will then perform DAD for the MN's RCoA on its subnet. If successful, the MAP will return a Binding Acknowledgement (BA) to the MN indicating a successful registration. Otherwise, the MAP MUST return a BA with the appropriate fault code. No new error codes are needed for this operation.

The MN MUST register its new RCoA with its HA by sending a BU that specifies the binding (RCoA, Home Address) as in MIPv6 (The home address field of the BU is set to the Home Address. An alternate-CoA sub-option is used and set to the RCoA). It can also send a similar BU (i.e. that specifies the binding between the Home Address and the RCoA) to its current CNs. Alternatively, if the I flag is set, the MN MAY use its RCoA as a source address for the BU. In this case no alternate-CoA suboption will be required.

If the P flag is set, the MN MUST use its RCoA as a source address when sending the BUs to the MAP, HA or CNs.

The MN SHOULD wait for the BA from the MAP before registering with its HA.
It should be noted that when binding the RCoA with the HA and CNs, the binding lifetime MUST NOT be larger than the MNs binding lifetime with the MAP, received in the Binding Acknowledgement.

In order to speed up handoff between MAPs, a MN may send a BU to its previous MAP specifying its new LCoA. Packets in transit that reach the previous MAP are then forwarded to the new LCoA.

The MAP will receive packets addressed to the MN's RCoA (from the HA or CNs). Packets will be tunnelled from the MAP to the MN's LCoA. The MN will de-capsulate the packets and process the packet in the normal manner.

When the MN moves locally (i.e. its MAP does not change), it MUST only register its new LCoA with its MAP. In this case, the RCoA stays unchanged.

Note that a MN can send a BU containing its LCoA (instead of its RCoA) with CNs who share the same link. Packets will then be routed directly without going through the MAP.

A MN and a network operator may prefer to hide the MNs LCoA from nodes outside the MAP domain. To ensure this, a MAP option can be sent with the P flag set. In this case, the mobile node MUST use its RCoA as the source address of its BU (no alternate-CoA sub-option is needed) to its HA and CNs. It MUST also use its RCoA as the source address for its outgoing packets. However, to support such feature ingress filtering on RCoA prefix(es) should not be done by the ARs.

On the other hand, a MN may prefer to hide its location from the CNs it communicates with and the HA. To achieve this, the MN should ensure that it does not provide its identity and location to any of the CNs. Since the implied identity of the MN is included in every packet (A Home Address), the MN should ensure that it does not provide its exact location to the CNs and HA. Hence, the MN should

use its RCoA as a source address for all its outgoing packets. This can be done if the I or P flags are set in the MAP option. Otherwise location privacy can not be provided in this manner.

6.2 MAP Operations

In this mode, a MAP acts exactly like a HA. It intercepts all packets addressed to registered Mobile Nodes and tunnels them to the corresponding LCoA.

A MAP operating in Basic mode would have no knowledge of the MN's Home address. The MN will send a BU to the MAP with the M, A and D flags set. The aim of this BU is to inform the MAP that the MN has formed an RCOA (contained in the BU as a Home address) and request that a MAP performs DAD on its behalf. This is identical to the HA operation in [1]. If the operation was successful, the MAP MUST respond with a BA to the MN indicating a successful operation. Otherwise a BA is sent with the appropriate error code. No new error codes are introduced for HMIPv6.

The MAP then acts as a HA for the RCoA. Packets addressed to the RCOA are intercepted by the MAP, using proxy Neighbour Advertisement, encapsulated and routed to the MNs LCoA.

6.3 HA Operations

The support of basic mode in HMIPv6 is completely transparent to the HA operation. Packets addressed to a MN s Home Address will be forwarded by the HA to its RCoA as described in [1].

6.4 CN Operations

Both HMIPv6 modes are completely transparent to CNs.

6.5 Local Mobility Management optimisation within a MAP domain

In [1], it is stated that short-term communication, particularly communication that may easily be retried upon failure, the mobile node MAY choose to directly use one of its care-of addresses as the source of the packet, thus not requiring the use of a Home Address option in the packet. Such use of the CoA will reduce the overhead of sending each packet due to the absence of additional options. In addition, it will provide an optimal route between the MN and CN.

With HMIPv6 Basic mode, if the I or P flags are set, a mobile node MAY choose to use its RCoA as the source of its packets without using a Home Address option, and to register the binding between its LCoA and RCoA with the local MAP.
As a result the MN is seen by the CN as a fixed node while moving within a MAP domain.

This use of the RCoA can be useful as it does not have the cost of Mobile IP (i.e. no bindings are sent over the Internet) but still provides some local mobility management to the MNs. Although, such use of RCoA does not provide global mobility (i.e. communication is broken when a mobile host moves to a new MAP), it would be useful for several applications communicating with other nodes for some period of time depending on the size of a MAP domain and the speed of the MN. Furthermore, since the support for BU processing in CNs is not mandated in [1], this mechanism can provide a way of obtaining route optimisation without sending BUs to the CNs.

6.6 Location Privacy

With HMIPv6 Basic mode, a mobile node MAY choose to hide its LCoA from its corresponding nodes and its home agent by using its RCoA in the source field of the packets that it sends.
As a result, the location tracking of a mobile node by its corresponding nodes or its home agent is difficult since they only know its RCoA and not its LCoA.

7. Extended mode: Supporting Mobile Nodes and Mobile Networks

The Extended mode of operation can support both Mobile Nodes and Mobile networks.

In the Extended mode of operation, the MN is configured with an RCoA that is assigned to one of the MAPs interfaces. The RCoA is received in the MAP option. Hence, unlike Basic mode, in this mode of operation, the MN MUST NOT use its RCoA as a source address in its outgoing packets.

The Extended mode of operation is applicable to both MNs and Mobile Networks. This mode will allow MNs within a Mobile Network to receive traffic in a route optimised manner (without being forwarded by the HA) in cases where MNs are unable to be configured with a topologically correct address.

In this mode, a MN will receive the MAP option with the M flag set. The T and V flags MAY also be set. The use of these flags is described in chapter 7.1.1 below. If the MN is HMIPv6-aware, it SHOULD use the RCoA to update its HA and CNs. As in Basic mode, the binding lifetimes for BUs sent to the HA and CNs, MUST NOT be larger than the MNs binding with the MAP.

The MAP will need to know how the destination address in a packet corresponds to the registered Home Address of a MN. This would be clear when the packets are sent from a CN to the global Home Address of the MN or to the CoA with a routing header. However, if the HA tunnels packets with addresses other than the MN's Global Home Address (e.g. Site-local), of which the MAP would have no knowledge, the HA SHOULD add a routing header to the outer packet. This routing

header MUST use one of the MN's registered Home Addresses as the final destination. This will enable the MAP to tunnel the packet to the correct destination (i.e. the MN's LCoA).

In the case where a MN is also a router to which several MN's may be connected (e.g. a Personal Area Network), it may not be possible for such router to obtain a new network prefix within a visited network. Hence, MNs connected to such router will end up with topologically incorrect addresses. By having the Mobile Router (MR) act as a MAP within the visited network, MNs connected to it may use its CoA as an alternate-COA when registering with their HA and other CNs.
Hence, maintaining the IPv6 powerful aggregation of routes within the backbone, while receiving route-optimised packets sent to the MNs attached to the Mobile Router (i.e. MAP).

7.1 MN Operations

After MAP discovery has taken place, a MN can register with one or more MAPs. The MN performs this local registration by sending a BU to the MAP with the appropriate flags set.

The MN will send a BU to the MAP. The BU MUST include:

- The A and M flags set,
- The MNs Home Address in the Home Address field,
- The MN s..LCoA as the CoA.

The MN SHOULD wait for a BA from the MAP before sending the BU to the HA. When sending a BU to the HA, the MN MUST include:

- The LCoA as a source address,
- The Home Address in the Home Address field and,
- An alternate-CoA suboption containing its RCoA.

The Home Address contained in the MAP registration MUST be the same Home Address that will be sent in the Home Agent registration. If a MN sends different BUs for different Home Addresses (in case it has multiple Home Addresses), the same process MUST be performed first for the MAP registrations. This is essential to allow a MAP to forward packets to the right MN when they are tunnelled from the HA. The MN MUST have a prefix length of zero in its BUs to the HA. This stops the HA from forming home addresses for that MN on each link that the HA is connected to, thus ensuring consistency in the Binding Caches of both the MAP and HA for the MN.

When in a foreign network, a MN needs to know which path a packet has

taken from the CN to the MN. That is, whether triangular routing (via the HA), or route optimisation, was used. When using the RCoA, packets tunnelled by the HA to the MAP will be de-capsulated and then encapsulated again with the MAP's address as the source address of the outer header. Therefore a check on whether the packet was tunnelled by the HA will not be sufficient to decide whether route optimisation is required.

Hence, a check for the existence of a routing header in the inner packet (i.e. with CN as source address), where the MN's home address is the final address, will be sufficient to determine whether the path was route optimised or not.

If the routing header does not exist, the MN SHOULD send a BU with the appropriate information to initiate route optimisation. It should be noted that such check is generic and would apply to all use cases of MIPv6 including the different MAP modes of operation in this memo. Hence, this check need not be an additional implementation for this mode of operation and can be the only check in an implementation to determine whether a BU should be sent to a CN.

7.1.1 The MN connected to a Mobile Router with MAP functionality

The MN maybe connected to a Mobile Router (MR) acting as a MAP. In many cases it may not be feasible for the MR to acquire a topologically correct prefix every time it changes its IP access point within the Internet. However, the need still remains for MNs connected to the MR to be reached by other CNs in a route optimised manner (i.e. Without sending traffic through the HA).

The MR is in this scenario will act as a host and a router. It can be configured with an LCoA using IPv6 stateless or stateful mechanisms. This address can be used by MNs as an RCoA. Hence the MR will advertise its own MAP option including its CoA, as well as, other MAP options received from the AR it is attached to. The MRs MAP option MUST include:

- The M flag set to inform the MN of the extended mode of operation
- The T flag set to indicate that the prefix on-link is not topologically correct.

If a MAP, further up in the hierarchy (fixed MAP), is advertised in addition to the MR, the MN should check the mode of operation of such MAP. If the MAP is operating in Basic mode, the MN should form an RCoA based on this MAP s option. Following this action, the MN should send a BU to the MR to bind its RCoA (obtained from the fixed MAP) to its address configured from the prefix received from the MRs router advertisement. The BU to the MR MUST include:

- The MN s address in the source address field. This address maybe the MNs Home Address,
- The M and A flags set,

- The RCoA (from the fixed MAP) in the Home Address field.

Following a successful binding, the MN MUST send a BU to the fixed MAP including:

- The source address as the MN s address if the V flag was set. If the V flag was not set, the source address field MUST contain the MRs LCoA. This is an exception of the rule mentioned in chapter 7.1 about the use of an RCoA as a source address. However, in this case this exception is needed to avoid any potential ingress filtering problems,
- The M and A flags set,
- The RCoA (from the fixed MAP) in the Home Address field.

If the RCoA was refused by the fixed MAP, the MN MUST re-send the BU to the MR with another RCoA based on the fixed MAP s prefix advertised.

In the case where the fixed MAP is operating in Extended mode, the MN is not required to send a BU to the MR as it will be able to recognise that the MNs address is on-link.

Finally the MN MUST send a BU to its HA including its RCoA (obtained from the upper MAP) as a CoA. The decision whether RCoA

7.2 HA Operations

In this mode of operation, the Home Agent operations are affected in a minor way. The only impact due to this HMIPv6 mode on the HA implementation is that when tunnelling packets to the MN with a site-local scoped home address, the HA SHOULD include a routing header in the outer packet with the MN's registered global home address as the final destination. This is done to enable the MAP to find the right routing entry for the MN, since it has no knowledge of Home addresses for which it received no BUs from the MN (e.g. Site-local home address).

7.3 MAP Operations

The MAP operation is in many ways similar to the HA operation described in [1] with some modifications. Upon reception of a BU from a MN with the M flag set, and provided it is allowed to accept this message (i.e. no local policy restrictions) the MAP MUST process the BU and if successful, add the information to its Binding Cache.

The BU from the MN will contain its LCoA as a source address and its Home address. A MAP MUST first check if the MN is authorised to use the MAP in this mode. If so, the MAP SHOULD process the BU in the normal manner.

If the A flag was set, the MAP MUST send a BAck to the MN.

All packets directed to the MN will be received by the MAP and tunnelled to the MN. Upon reception of an encapsulated packet, from a MNs HA, with no routing header in the outer packet, the packet is de-capsulated in the normal way. If the inside packet contains a destination address that doesn't belong to the MAP, the MAP should check its Binding Cache to see if the address belongs to any of its registered MN's. If it does, the packet MUST be tunnelled to the MN's registered LCoA. Otherwise, the packet is processed in the normal way.

If the received encapsulated packet contains a routing header, the MAP MUST process the routing header in the normal way. After processing the routing header, the MAP MUST check whether the final destination corresponds to an entry in its binding cache. If it does, the MAP MUST tunnel the packet to the MN's LCoA.

When a packet containing a routing header is received (from a CN) the routing header is processed as usual and the packet is then encapsulated to the MN.

If the MAP option allows for reverse tunnelling from the MN (i.e. the V flag is set), it MUST set a bi-directional tunnel to the MN upon reception of a Binding Update.

7.3.1 The MAP as an MR

If the MAP is an MR with one or more MNs connected on one interface, and an AR on the other interface. When changing ARs, the MAP MUST advertise its own MAP option as well as other MAP options received from the AR. The MRs MAP option would contain its own LCoA. This would allow the MNs to obtain a new topologically correct RCoA and update the higher MAP in the hierarchy.

While operating as an MR, and provided a fixed MAP allowing reverse tunnelling (V flag set) exists, the MR MUST tunnel all outgoing packets from MNs connected to it, to the fixed MAP located further in the hierarchy.

7.4 CN Operations

In this mode, HMIPv6 is transparent to CNs.

8. Comparison between the HMIPv6 modes of operation

In this memo two different modes of operation are defined for HMIPv6 which will affect the MN s choice of its COA when located in a foreign network. As shown above the selection of the mode of

operation is done based on the information sent in the MAP option. Such information MUST be configurable by the network administrator. To simplify MN and MAP implementations, only one mode can be used by the MAP at a time.

The use of Basic mode is simple as it is completely independent of the HAs implementation. Packets are intercepted by the MAP (using a HA implementation) and encapsulated again to the MN. On the other hand, if Extended mode is used, the MAP will de-capsulate the packets and then encapsulate them again to the MN.
Hence, in the latter case, only one additional IPv6 header is needed for packets routed through the HA, as opposed to two headers in the former. If an appropriate header compression mechanism is used, this may not be an issue. However, if no header compression is used, it is more efficient to use the Extended mode of operation.

Another aspect of the comparison, is the Duplicate Address Detection (DAD) required when performing the initial registration with the MAP. If Basic mode is used, the MAP MUST perform DAD for the RCoA. On the other hand, if extended mode is used, there will be no need to

perform DAD as the BU sent to the MAP will bind the MNs home address to the LCoA. Since no DAD for the LCoA is required by the MAP, the registration can be faster when using Extended mode. This aspect of the comparison may be less significant if no inter-MAP handoffs are expected when roaming within the visited network (i.e. one MAP domain in the visited network). However, if inter-MAP handoffs are expected, the time taken to perform DAD by the MAP may become significant.

In Basic mode, to avoid DAD delays during inter-MAP mobility, the MN MAY register its new LCoA with its previous MAP. Packets will be redirected from the previous MAP to the new LCoA while DAD is performed. In this scenario the time taken to perform DAD by the MAP might not become significant.

9. Smooth Handoff

A MAP should be able to handle smooth handoffs. When a mobile host moves into a new MAP domain, the MN may send a BU to the previous MAP requesting to forward packets addressed to the MN s new CoA. This is similar to the smooth handoff mechanism of Mobile IPv6.

10. Special optimisations for sending BUs

In some link layers that require some L2 signalling before sending each frame, it maybe useful for MNs to encapsulate the BU sent to the HA inside the BU sent to the MAP. The decision on whether this optimisation should be used or not is left to the MN implementation, depending on the type of underlying L2 used for transmission.

It should be noted however, that the use of such encapsulation may cause extra signalling in case the Home registration was rejected by

the HA or MAP (e.g. if DAD failed and the MN s required to provide a new Home address or if the MAP rejected the BU, forcing the MN to re-register with the HA).

11. Notes on MAP selection by the MN

HMIPv6 provides a very flexible mechanism for local mobility management within a visited network. As explained earlier a MAP can exist on any level in a hierarchy including the AR. Several MAPs can be located within a hierarchy independently of each other. In addition, overlapping MAP domains are also allowed and recommended. Both static and dynamic hierarchies are supported for either mode of operation. Hence, the discussion below is independent of the MAPs mode of operation.

When the MN receives a router Advertisement including a MAP option, it should perform actions according to the following movement detection mechanisms. In a Hierarchical Mobile IP network such as the one described in this draft, the MN SHOULD be:

- "Eager" to perform new bindings
- "Lazy" in releasing existing bindings

The above means that the MN should register with any "new" MAP advertised by the AR (Eager).
The method by which the MN determines whether the MAP is a "new" MAP is described in chapter 5 above. The MN should not release existing bindings until it no longer receives the MAP option or the lifetime of its existing binding expires (Lazy).
This Eager-Lazy approach described above will assist in providing a fallback mechanism in case one of the MAP routers crash as it would reduce the time it takes for a MN to inform its CNs and HA about its new COA.

11.1 MAP selection in a distributed-MAPs environment

For a MN to select one or more MAPs, where several MAPs are available in the same domain, in an optimised manner, several factors need to be considered.

Except for the case of a Mobile network connected via an MR to an AR, there are no benefits foreseen in selecting more than one MAP and forcing packets to be sent from the higher MAP down through a hierarchy of MAPs. This approach may add delays and eliminate the robustness of IP routing between the highest MAP and the MN. Hence, allowing more than one MAP (above the AR) within a network should not imply that the MN forces packets to be routed down the hierarchy of MAPs. However, placing more than one MAP above the AR can be used for redundancy and as an optimisation for the different mobility scenarios experienced by MNs.

In terms of the Distance based selection in a network with several MAPs, a MN may choose to register with the furthest MAP to avoid frequent re-registrations. This is particularly important for fast MNs that will perform frequent handoffs. In this scenario, the choice of a further MAP would reduce the probability of having to change a MAP and informing all CNs and the HA.

In the case of Mobile networks, connected via an MR to another network, MNs should bind their MRs CoA (advertised in the MR s MAP option) to their Home addresses. For example, in this case the MN may receive two MAP options, one including the MRs address (MAP1) and another for a MAP further away in the hierarchy of routers (MAP2). The MN should then send a BU to MAP2 binding its Home address to the MR.

In a scenario where several MAPs are discovered by the MN in one domain, the MN may need some sophisticated algorithms to be able to select the appropriate MAP. These algorithms would have the MN speed as an input (for distance based selection) combined with the preference field in the MAP option.

However, this memo proposes that the MN uses the following algorithm as a default one, where other optimised algorithms may not be available. The following algorithm is simply based on selecting the furthest possible MAP, provided that its preference value did not reach the maximum value of 15. The MN operation is shown below:

1. Receive and parse all MAP options
2. Arrange MAPs in a descending order, starting with the furthest MAP
3. Select furthest MAP, based on the distance
4. If the Preference value is set to 15, select the following MAP in the list.
5. Repeat step (4) while new MAP options still exist.

Implementing the steps above would result in MNs selecting the furthest possible MAP by default. This will continue to take place, until the preference value reaches the maximum (15). Following this, MNs will start selecting another MAP.

11.2 MAP selection in a flat mobility management architecture

Network operators may choose a flat architecture in some cases where a MIP handoff may be considered a rare event. In these scenarios operators may choose to include the MAP function in ARs only. The inclusion of the MAP function in ARs can still be useful to reduce the time required to update all CNs and the HA. In this scenario, a MN may choose a MAP (in the AR) as an anchor point when performing a handoff. This kind of dynamic hierarchy (or anchoring) is only recommended for cases where inter-AR movement is not frequent.

12. Security considerations

HMIPv6 does not introduce more security problems than Mobile IPv6.

A mobile host has to register with its HA and with the Mobility Anchor Point. All BUs between the MN and the MAP MUST be authenticated as per MIPv6. This means that the mobile host has to share an authentication key (private or public) with all MAPs it may visit. These keys can be pre-installed manually or obtained dynamically via IKE, AAA servers or other mechanisms. The Security association establishment between the MN and the MAP MUST be based on the Home address when using the extended mode, and the RCoA when using the basic mode.

13. Acknowledgements

The authors would like to thank Conny Larsson (Ericsson) and Mattias Pettersson (Ericsson) for their valuable input to this draft.

The authors from INRIA would also like to thank the members of the French RNRT MobiSecV6 project (BULL, France Telecom and INRIA) for testing our implementation and for their valuable feedback. They

would also like to thank the French Governement for partially funding this project.

In addition, the authors would like to thank the following members of the working group in alphabetical order: Samita Chakrabarti (Sun), Gopal Dommety (Cisco), Eva Gustaffson (Ericsson), Dave Johnson (Rice University), Annika Jonsson (Ericsson), James Kempf (Sun), Fergal Ladley, Erik Nordmark (Sun), Basavaraj Patil (Nokia) and Alper Yegin (Sun) for their comments on the draft.

14. Notice Regarding Intellectual Property Rights

see http://www.ietf.org/ietf/IPR/ERICSSON-General

15. References

[1] D. Johnson and C. Perkins, "Mobility Support in IPv6", draft-ietf-mobileip-ipv6-13.txt, February 2000.

[2] E. Gustafsson et al, "Mobile IP Regional Tunnel Management", draft-ietf-mobileip-reg-tunnel-05. Work in progress March 2000.

[3] K. ElMalki, Editor, et al, "Low latency Handoffs in Mobile IPv4", draft-ietf-mobileip-lowlatency-handoffs-v4-00. work in progress.

[4] G. Tsirtsis, Editor, et al,"Fast Handovers for Mobile IPv6", draft-ietf-mobileip-fast-mipv6-00.txt. Work in progress.

[5] M. Crawford Router Renumbering for IPv6 . RFC 2984.

[6] S. Thomson and T. Narten "IPv6 Stateless Address Autoconfiguration". RFC 2462.

[7] T. Narten, E. Nordmark and W. Simpson Neighbour Discovery for IP version 6 . RFC 2461.

[8] E. Nordmark, Site prefixes in Neigbour Discovery . draft-ietf-ipng-site-prefixes-05. Work in progress.

[9] K. ElMalki and H. Soliman, Simultaneous Bindings for Mobile IPv6 Fast Handoffs . draft-elmalki-mobileip-bicasting-v6-01. Work in progress.

16. Authors' Addresses

The working group can be contacted via the current chairs:

Basavaraj Patil
Nokia Corporation

Phil Roberts
Motorola M/S M8-540

6000 Connection Drive
Irving, TX 75039
USA

Phone: +1 972-894-6709
EMail: Raj.Patil@nokia.com
Fax : +1 972-894-5349

1501 West Shure Drive
Arlington Heights, IL 60004
USA

Phone: +1 847-632-3148
EMail: QA3445@email.mot.com

Questions about this memo can also be directed to:

Hesham Soliman
Ericsson Radio Systems AB
Torshamnsgatan 23,
Kista, Stockholm 16480
SWEDEN

Phone: +46 8 4046619
Fax: +46 8 4047020
E-mail: Hesham.Soliman@era.ericsson.se

Claude Castelluccia
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
France

email: claude.castelluccia@inria.fr
phone: +33 4 76 61 52 15
fax: +33 4 76 61 52 52

Karim El Malki
Ericsson Radio Systems AB
LM Ericssons Vag. 8
126 25 Stockholm
SWEDEN

Phone: +46 8 7195803
Fax: +46 8 7190170
E-mail: Karim.El-Malki@era.ericsson.se

Ludovic Bellier
INRIA Rhone-Alpes
655 avenue de l'Europe
38330 Montbonnot Saint-Martin
France

email: ludovic.bellier@inria.fr
phone: +33 4 76 61 52 15
fax: +33 4 76 61 52 52

17. Appendix A Fast Mobile IPv6 Handovers and HMIPv6

Fast Handovers are required to ensure that the layer 3 (Mobile IP) handover delay is minimised, thus also minimising and possibly eliminating the period of service disruption which normally occurs when a MN moves between two ARs. This period of service disruption usually occurs due to the time required by the MN to update its HA using Binding Updates after it moves between ARs. During this time period the MN cannot resume or continue communications. The mechanism to achieve Fast Handovers with Mobile IPv6 is described in [4] and is briefly summarised here. This mechanism allows the anticipation of the layer 3 handover such that data traffic can be redirected to the MN s new location before it moves there.

While the MN is connected to its old Access Router (oAR) and is about to move to a new Access Router (nAR), the Fast Handovers in Mobile IPv6 requires in sequence:

1) the MN to obtain a new care-of address at the nAR while connected to the oAR
2) New CoA to be used at nAR case: the MN to send a F-BU (Fast BU) to its old anchor point (i.e. oAR) to update its binding cache with the MNs new CoA while still attached to oAR
3) The old anchor point (i.e. oAR) to start forwarding packets destined for the MN to the MN s new CoA at nAR (or old CoA tunnelled to nAR if new CoA is not applicable).
4) Old CoA to be used at nAR case: the MN to send a F-BU (Fast BU) to its old anchor point (i.e. oAR), after it has moved and attached to nAR, in order to update its binding cache with the MNs new CoA.

The MN or oAR may initiate the Fast Handover procedure by using wireless link-layer information or link-layer triggers which inform that the MN will soon be handed off between two wireless access points respectively attached to oAR and nAR. If the trigger is received at the MN, the MN will initiate the layer-3 handover process by sending a Proxy Router Solicitation message to oAR. Instead if the trigger is received at oAR then it will transmit a Proxy Router Advertisement to the appropriate MN, without the need for solicitations. The basic Fast Handover message exchanges are illustrated in Figure A.1.

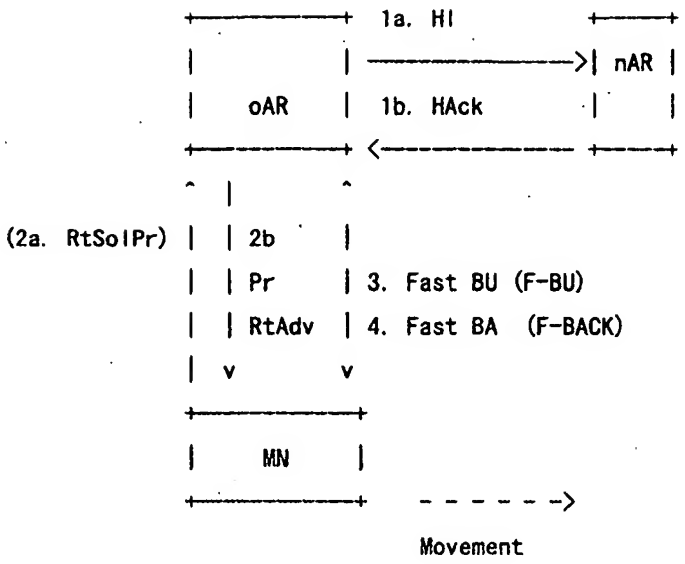


Figure A.1 Fast MIPv6 Handover Protocol

The MN obtains a new care-of address while connected to oAR by means of router advertisements containing information from the nAR (Proxy Router Advertisement which may be sent due to a Proxy Router Solicitation). The oAR will validate the MN s new CoA by sending a Handover Initiate (HI) message to the nAR. The new CoA sent in the HI message is formed by appending the MNs current interface identifier to the nAR s prefix. Based on the response generated in the Handover Acknowledge (HAck) message, the oAR will either generate a tunnel to the MNs new CoA (if the address was valid) or generate a tunnel to the nAR s address (if the address was already in use on the new subnet). If the address was already in use on the new subnet it is assumed that there will be no time to perform another attempt to configure the MN with a CoA on the new link, so the nAR will generate a host route for the MN using its old CoA. Note that message 1a may

precede message 2b or occur at the same time.

In [4], the ARs act as local Home Agents which hold binding caches for the MNs and receive Binding Updates. This makes these ARs function like the MAP specified in this document. Also, it is quite possible that the ARs are not directly connected, but communicate through an aggregation router. Such an aggregation router is therefore also an ideal position for the MAP functionality. These are two ways of integrating the HMIPv6 and Fast Handover mechanisms. The first involves placing MAPs in place of the ARs which is a natural step. The second scenario involves placing the MAP in an aggregation router above the ARs. In this case, [4] specifies forwarding of packets between oAR and nAR. This could be inefficient in terms of delay, bandwidth efficiency since packets will traverse the MAP-oAR link twice and packets arriving out of order at the MN. Using the MAP in the aggregation router would improve the efficiency of Fast Handovers which could make use of the MAP to redirect traffic, thus saving delay and bandwidth between the aggregation router and the oAR.

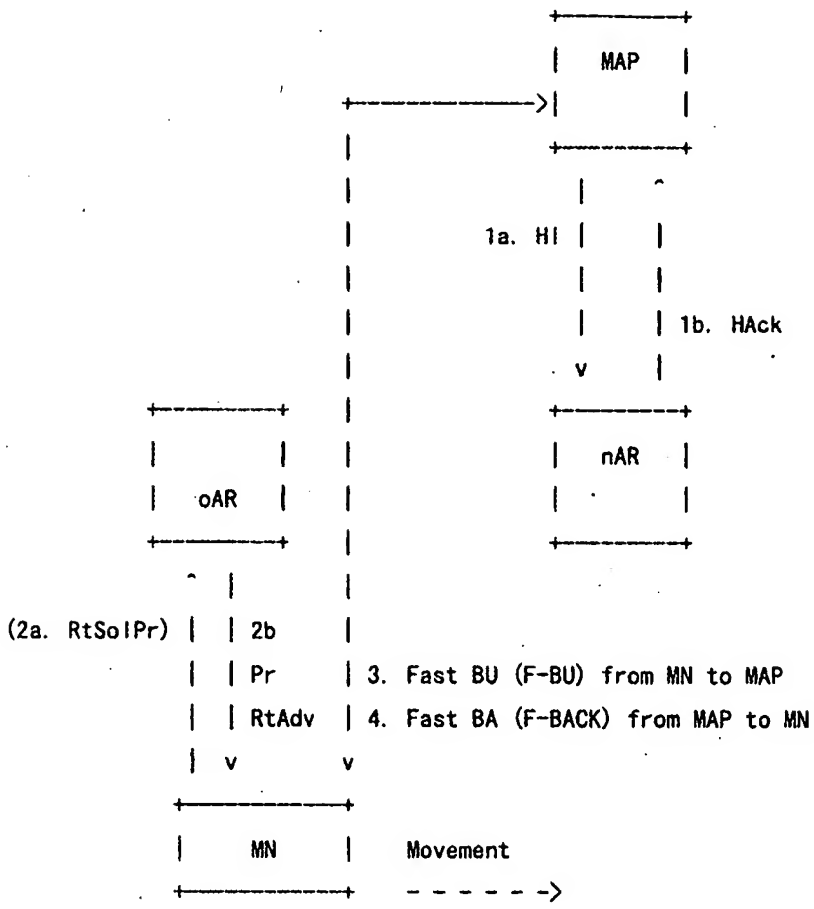


Figure A.2 Fast MIPv6 Handover Protocol using HMIPv6

In Figure A.2, the HI/HAck messages now occur between the MAP and nAR to check the validity of the newly requested care-of address and to establish a temporary tunnel should the new care-of address not be valid. Therefore the same functionality of the Fast Handover procedure is kept but the anchor point is moved from the oAR to the MAP.

As in the previous Fast Handover procedure, in the network-determined case the layer-2 triggers at the oAR will cause the oAR to send a Proxy Router Advertisement to the MN with the MAP option. In the mobile-determined case this is preceded by a Proxy Router Solicitation from the MN. The same layer-2 trigger at oAR in the network-determined case could be used to independently initiate Context Transfer (e.g. QoS) between oAR and nAR. In the mobile-determined case the trigger at oAR could be replaced by the reception of a Proxy Router Solicitation or F-BU. Context Transfer is being worked on in the IETF Seamoby WG [CT].

The combination of Fast Handover and HMIPv6 allows the anticipation of the layer 3 handoff such that data traffic can be efficiently redirected to the MN s new location before it moves there. However it is not easy to determine the correct time to start forwarding traffic from the MAP to the MNs new location, which has an impact on how smooth the handoff will be. The same issues arises in [4] with respect to when to start forwarding between oAR and nAR. Packet loss will occur if this is performed too late or too early with respect to the time in which the MN detaches from oAR and attaches to nAR. Such

packet loss is likely to occur if the MAP updates its binding cache upon receiving the anticipated F-BU, since it is not known when exactly the MN will perform or complete the layer-2 handover to nAR relative to when the MN transmits the F-BU. Also, some measure is needed to support the case in which the MNs layer-2 handover unexpectedly fails (after Fast Handover has been initiated) or when the MN moves quickly back-and-forth between ARs (ping-pong). Simultaneous bindings [9] provides a solution to these issues. In [9] a new Simultaneous Bindings Flag is added to the Fast Binding Update (F-BU) message and a new Simultaneous Bindings suboption is defined for Fast Binding Acknowledgement (F-BAck) message. Using this enhanced mechanism, upon layer-3 handover, traffic for the MN will be sent from the MAP to both oAR and nAR for a certain period thus isolating the MN from layer-2 effects such as handover timing, ping-pong or handover failure and providing the MN with uninterrupted layer-3 connectivity.

18. Appendix B. Support for Mobile Networks

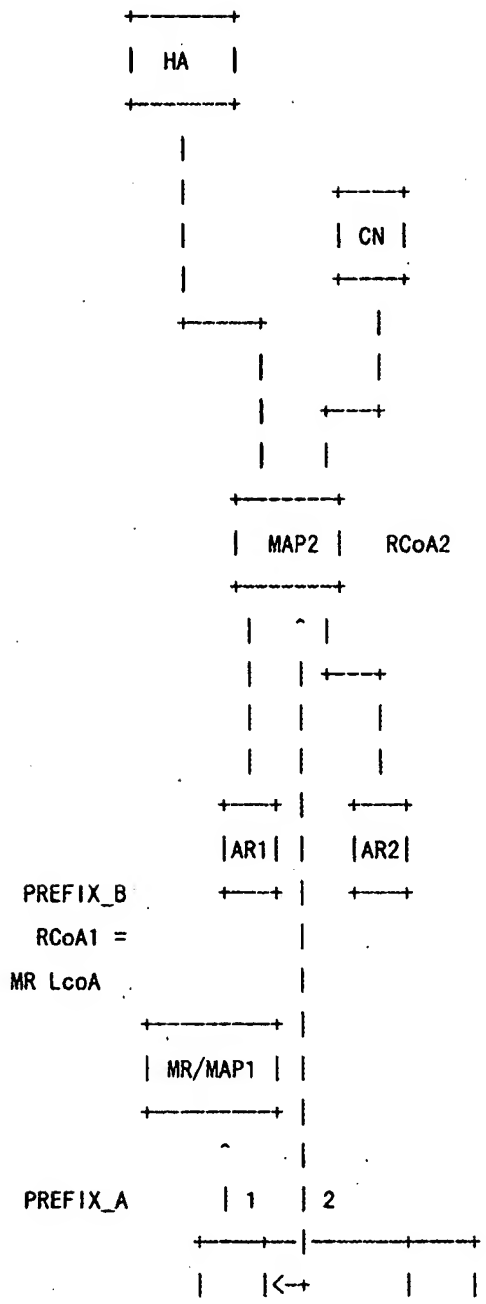
The Extended mode of operation for HMIPv6 allows for a mechanism by which MNs connected to a roaming MR can receive packets in a route optimised manner. This is achieved by adding the Extended mode functionality to the MR, as decribed in chapter 7. Another approach may provide mechanisms allowing a MR to send a prefix-scoped Binding update to its HA to allow it to forward all packets addressed to the MR s prefix. While this approach would allow MNs connected to the MR to be reachable (even if they belong to another HA), it does not allow them to be reachable in a route optimised manner. Packets destined to the MNs will be received by their HA (may or may not be the MRs HA), encapsulated to the MR s HA and re-encapsulated to the MRs CoA.
Prefix-scoped BUs maybe better suited to mobile networks where some nodes do not implement the MN functionality, or for other network mobility scenarios where a large mobile network (in a train or plane) is connected to the Internet via a low Bandwidth link and is frequently moving between ARs. In the latter case, prefix-scoped BUs would reduce the number of BUs sent each time the mobile network moves to 1 BU.

When using HMIPv6 s Extended mode, MNs will become aware of the MRs movement within the topology and consequently will send a BU to its HA (or local MAP within the domain) whenever the MR changes its L3 attachment point. Hence, MNs will be able to receive route optimised packets from CNs, provided that such CNs can process the MN s BU.

It should be noted that the use of HMIPv6s Extended mode can coexist with prefix-based binding updates. For instance, a MR, being a MAP, can also send a prefix-scoped BU to its HA to allow it to forward all

packets to its CoA. In the mean time it can advertise its own MAP option to allow HMIPv6-aware MNs to receive an RCoA and update their respective CNs

In this appendix an example of a mobile network is given. The MN and MR operations are shown for this example.
Figure B.1 shows an example of a mobile network.


HA
CN
MAP2
RCoA2
AR1
AR2
PREFIX_B
RCoA1 =
MR LcoA
MR/MAP1
PREFIX_A
1
2

B.1. An example of a Mobile network

example shown above, an MR is attached to AR1. AR1 is
ising PREFIX_B. The MR is receiving PEFIX_B on the interface
ed to AR1 and based on this prefix, the MR forms its LCoA.
is also configured on another interface (connected to th MNs)
ertise PREFIX_A, where PREFIX_A does not belong to the same
as PREFIX_B. Hence, it may not be possible to use addresses
on PREFIX_A as source addresses for the MNs. Furthermore, the
that the MR is currently connected to will not advertise
oility to PREFIX_A to maintain route aggregation in the
ne.

for the MN to be reachable in a direct way (route optimised)
CNs, the MN will use the MRs LCoA as an RCoA included as an
ite-CoA in its BUs to the HA and CNs.